

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Information associated with Temaj.bess@icloud.com
that is stored at premises owned, maintained,
controlled, or operated by Apple Inc.

Case No. 23-M-681

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. § 371; 922(a)(1);
922(a)(6); 922(g)(1); 922 (k);
922 (o)

Offense Description
Conspiracy; Dealing firearms w/out license; Lying & buying; Unlawful possession
of firearms & ammunition by convicted felon; Receiving/ship/transport of a firearm
with an obliterated serial number; transfer or possession of machinegun

The application is based on these facts:

See Affidavit

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Sean Carlson, ATF SA

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
(specify reliable electronic means).

Date:

9/21/2023

City and state: Green Bay, Wisconsin

Judge's signature

Honorable Magistrate Judge Sickel

Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Sean Carlson, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises owned, maintained, controlled, or operated by Apple Inc. ("Apple"), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am employed as a Special Agent with the United States Department of Justice, Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF") assigned to the Milwaukee Field Office since November 2015. I have been employed as a full-time law enforcement officer for approximately fifteen years. Prior to my employment at ATF, I was a Patrol Officer at the Hammond Police Department in Hammond, Indiana for over four (4) years, and then I served approximately five (5) years as a Federal Air Marshal with the U.S. Department of Homeland Security.

3. As a Special Agent, I have participated in the investigation of firearms and

narcotics-related offenses, resulting in the prosecution and conviction of numerous individuals and the seizure of illegal drugs, and weapons. As a firearms investigator, I have interviewed many individuals involved in firearm and drug trafficking and have obtained information from them regarding acquisition, sale, importation, manufacture, and distribution of firearms and controlled substances. Through my training and experience, I am familiar with the actions, habits, traits, methods, and terminology utilized by the traffickers and abusers of controlled substances.

4. Based on my training, experience and participation in drug trafficking and firearms trafficking investigations, I know and have observed the following:

5. I have relied on informants to investigate firearms trafficking and drug trafficking. Through informant interviews and debriefings of individuals involved in those offenses, I have learned about the manner in which individuals and organizations finance, purchase, transport, and distribute firearms and narcotics both within and outside of Wisconsin. I have utilized informants to conduct "controlled purchases" of firearms and controlled substances from individuals, as opposed to licensed gun dealers. I have also conducted surveillance of individuals engaged in firearms and drug trafficking and participated in the execution of numerous search warrants resulting in the seizure of drugs, firearms, ammunition, and magazines.

6. Based on my training and experience, I have become familiar with the language utilized over the telephone to discuss firearms and drug trafficking and know that the language is often limited, guarded, and coded. I also know that firearms and drug traffickers often use electronic devices (such as computers and cellular phones) and social media to facilitate these crimes. Based on my experience, I know that

firearms traffickers may keep photographs of these items on electronic devices.

7. I also know that drug traffickers and firearms traffickers commonly possess—on their person, at their residences, at their places of business, in their vehicles, and other locations where they exercise dominion and control—firearms, ammunition, and records or receipts pertaining to such.

8. I know that firearms traffickers and drug traffickers often put their telephones in nominee names to distance themselves from telephones that are utilized to facilitate these and related offenses. I also know that firearm and drug traffickers often use proceeds to purchase assets such as vehicles, property, jewelry, and narcotics. I also know that firearm and drug traffickers often use nominees to purchase or title these assets to avoid scrutiny from law enforcement.

9. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other investigators and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

10. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 922(a)(1) (dealing firearms without a license), 18 U.S.C. § 922(a)(6) (lying and buying), 18 U.S.C. § 922(g)(1) (unlawful possession of firearms and ammunition by a convicted felon), 18 U.S.C. § 922 (k) (receiving/ship/transport of a firearm with an obliterated serial number), and 18 U.S.C. § 922 (o) (transfer or possession of machinegun) have been committed and that evidence of those violations

is contained in following Apple iCloud account:

- Temaj.bess@icloud.com

which is linked to the owner, Temaj BESS. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

JURISDICTION

11. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

12. On March 16, 2023, Appleton Police Department (PD) arrested Jeremiah D. RANDOLPH (B/M, DOB 03/17/2004) for felon in possession of a firearm pursuant to a state of Wisconsin (act 79) search conducted by RANDOLPH’s probation agent. It should be noted, RANDOLPH is prohibited from possessing firearms based on previous state of Wisconsin felony convictions for bail jumping.

13. During the Act 79 search of RANDOLPH's residence, RANDOLPH’s probation agent located a firearm with an obliterated serial number, which was turned over to Appleton PD. Appleton PD Sgt. Michael Chevremont arrested RANDOLPH for the located firearm, and during a mirandized interview with Appleton PD, RANDOLPH stated he received the firearm from a subject named Temaj S. BESS (B/M, DOB 02/06/2001) in Fall of 2022. RANDOLPH stated he asked BESS to purchase the firearm on his behalf, because he wanted it for personal protection. RANDOLPH stated

he stopped carrying the firearm outside of his residence, after co-workers warned him it was illegal for him to possess a firearm. RANDOLPH further stated he went with BESS to the Federal Firearms Licensee (FFL) when BESS purchased the firearm, and RANDOLPH paid approximately \$200 to BESS, in order for BESS to purchase the firearm. RANDOLPH stated BESS lived on "Newberry Street" in Appleton, WI

14. The recovered firearm is more particularly described as a Taurus pistol (model G2C, 9 mm, with an obliterated serial number).

15. Following the interview with RANDOLPH, Appleton PD Sgt. Chevremont went to Federal Firearms Licensee (FFL) Mister Money, located at 1933B N. Richmond Street, Appleton, Wisconsin and retrieved surveillance camera footage for the purchase, which occurred on October 25, 2022. Review of the footage depicts a subject matching BESS' physical description and a person Sgt. Chevremont recognized as RANDOLPH at the store with BESS. RANDOLPH is observed looking at the firearms and pointing to the firearms in the case prior to BESS completing the ATF Form 4473 background paperwork and BESS purchasing the firearm.

16. The firearm involved in this purchase is more particularly described as a Taurus pistol (model G2C, 9 mm, bearing serial no. ACB600569).

17. On March 23, 2023, Appleton PD Sgt. Chevremont called the user of cellular phone number 773-220-3134, and the subject verbally identified themselves as Temaj BESS. Sgt. Chevremont arranged for BESS to come to Appleton PD later that day for an interview. During the recorded interview, BESS stated he has previously purchased approximately seven (7) firearms, but he stated they were all currently missing and no longer in his possession. BESS stated his previous purchases included a

Glock pistol, Taurus pistol, and an unknown rifle. BESS stated he remembered the transaction for the aforementioned Taurus pistol at the FFL Mister Money, and he stated RANDOLPH was with him at the time of purchase. BESS stated he paid \$310 and he borrowed the money to buy the firearm from RANDOLPH. BESS stated he was buying the firearm for himself, but approximately one week after the purchase of the firearm he realized he would be unable to pay RANDOLPH back. BESS stated at this point he gave RANDOLPH the firearm. BESS stated he knew RANDOLPH was unable to legally purchase a firearm for himself because he was 18 years old at the time BESS gave RANDOLPH the pistol. BESS stated RANDOLPH paid him the funds for the firearm purchase via Cashapp. BESS stated he did not remove the serial number from the firearm.

18. During the interview with Sgt. Chevremonte, BESS stated he currently resides at 1820 E. Newberry Street, Appleton, WI.

19. It should be noted, on May 1, 2023, Your Affiant conducted a search of law enforcement databases and determined 773-220-3134 has been associated with Temaj BESS, through public records, from August 2019 to present.

20. In addition to the transaction with RANDOLPH, BESS stated he also bought a firearm for a subject named "Patrick WASSINK" at FFL Pawn America, located in Grand Chute, WI. BESS stated he also went to the FFL with WASSINK and he gave WASSINK the firearm immediately after the sale. It should be noted, Sgt. Chevremont later identified Patrick WASSINK as Patrick A. WATSON (DOB 07/04/2001).

21. During the interview with BESS, BESS stated to Sgt. Chevremont his

address was 1820 E. Newberry Street, Appleton, WI, which is located in the Eastern District of Wisconsin.

22. On April 19, 2023, your affiant queried ATF eTrace reports for law enforcement firearm traces associated Temaj BESS and located the following reports:

- **ATF eTrace Report no. T20230151063** which detailed Temaj BESS' purchase of a Taurus pistol (model G2C, 9 mm, bearing serial no. ACB600569) from FFL Mister Money on October 25, 2022. This firearm was recovered on March 16, 2023, in the possession of Jeremiah D. RANDOLPH. The time-to-crime was **142 days**.
- **ATF eTrace Report no. T20220566489**, which detailed Temaj BESS' purchase of a Taurus pistol (model G3C, 9 mm, bearing serial no. ADA795418) from FFL Fleet Farm, located at 3035 West Wisconsin Avenue, Appleton, Wisconsin, on May 05, 2022. This firearm was recovered on November 04, 2022, in the possession of Zacorian TURNER (DOB 07/24/2004). The time-to-crime was **183 days**.

23. Your affiant knows from information published by the ATF's Violent Crime Analysis Branch (as of June 16, 2016) the national average for a gun to be recovered in a crime by law enforcement after the original purchase date is 10.48 years (also known as "time to crime"). Additionally, the average time to crime of firearms in Illinois is **11.81 years** and **8.18 years** in Wisconsin. In your affiant's training and experience, a subject with law enforcement traces of multiple firearms with a low time-to-crime can be an indicator that the purchaser is engaged in firearms trafficking.

24. On or around April 14, 2023, Sgt. Chevremont observed on BESS' publicly visible Instagram profile username "lilgen5frmdaa" the following three photographs which depicted BESS holding an item in a manner consistent with someone holding a

firearm. The photographs had emoji placed over the item BESS was holding, so as to obscure the item.



25. Sgt. Chevremont previously identified this Instagram profile as belonging to BESS because the profile photograph and numerous photographs posted to the account depict BESS. Sgt. Chevremont also located a Facebook.com profile belonging to BESS which listed this Instagram account as belonging to him as well. Your affiant knows from training and experience that it is common for those engaged in firearms trafficking to utilize social media to advertise firearms they have for sale as well enhance their social stature within their peer group.

26. On April 19, 2023, Sgt. Chevremont interviewed Patrick WATSON, at the Appleton police department, regarding the firearm BESS stated he purchased. It should be noted, prior to this interview, Sgt. Chevremont determined using a law enforcement database that BESS purchased a Glock pistol (model Glock 19 Gen 5, 9 mm, bearing serial no. BUHK214) from Pawn America, located at 500 N. Westhill Boulevard, Grand Chute, Wisconsin, on September 7, 2022. During the interview, WATSON stated he knew BESS and both individuals hung out in the same friend group. WATSON stated

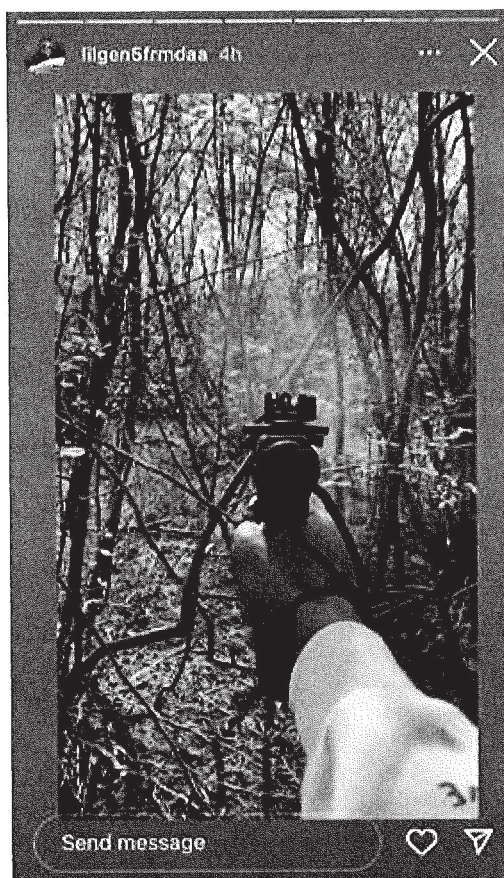
he purchased the aforementioned Glock pistol from BESS. WATSON stated before BESS purchased the Glock pistol, WATSON tried to purchase the same firearm directly from Pawn America. WATSON stated he completed the ATF Form 4473 for the firearm, but Pawn America did not call him back to complete the purchase. WATSON stated to Sgt. Chevremont he was unsure if he could legally purchase the firearm because he had been previously charged for felony crimes in Wisconsin as a juvenile. WATSON stated on September 7, 2022, the day BESS purchased the Glock pistol from Pawn America, WATSON met with a group of friends, including BESS. WATSON stated the group went to Pawn America together, and BESS purchased the firearm. WATSON stated BESS paid approximately \$500 for the pistol. WATSON stated he told BESS at the time of the purchase that he would buy the firearm from him for "a little bit more" than BESS paid for it. WATSON stated on that same date, he offered BESS \$650 or \$700 for the firearm and BESS agreed to sell it for that price. WATSON stated he went to his brother's house to get the money and met BESS later on September 7, 2022, and completed the purchase of the firearm from BESS. WATSON stated he took possession of the firearm less than a "couple hours" after BESS purchased the firearm and WATSON believed BESS could purchase the firearm for him because he was "legal".

27. In addition to describing the firearm transaction with BESS, WATSON stated his only point of contact with BESS was through BESS' Facebook account. WATSON also stated he knew BESS could legally purchase firearms because of previous conversations he had with BESS prior to the purchase on September 7, 2022. WATSON stated he did not know why BESS purchased the Glock that day because

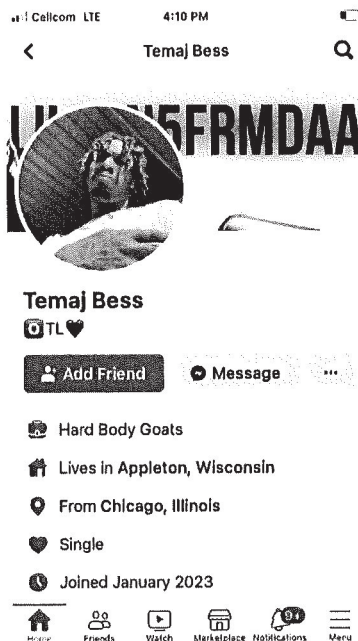
BESS already owned a firearm. WATSON also stated he knew BESS had previously purchased several other Glock pistols, but he had only seen him in possession of one. When asked where the other Glock pistols were, WATSON replied "I don't know. I know he bought me one"; however, he later corrected this statement by saying BESS bought the firearm for himself.

28. It should be noted, WATSON is federally prohibited from possessing a firearm and/or ammunition based on a state of Wisconsin juvenile felony conviction for robbery with use of force.

29. On or around May 11, 2023, Sgt. Chevremont observed on BESS' publicly visible Instagram profile username "lilgen5frmdaa" the following photograph depicting a what appears to be a black male with a tattoo on their right hand, firing a pistol in a wooded area.



30. It should be noted, your affiant is aware BESS has a prominent tattoo on his right hand in a location consistent with the hand depicted in the above Instagram photograph, leading him to believe BESS is likely the possessor of this firearm. See the below photograph from BESS' Facebook.com profile which depicts BESS and his tattooed right hand.



31. On May 9, 2023, the Honorable James R. Sickel, U.S. Magistrate Judge, signed a search warrant which allowed for the collection of real time location data for (773) 220-3134, the cellular telephone number associated with BESS. The warrant was executed with T-Mobile on May 10, 2023, and will expire on June 8, 2023.

32. Analysis of location data for (773) 220-3134, the number associated with BESS, collected between May 10, 2023 and June 6, 2023, indicated the phone associated with this number has been pinging on cellular towers which cover 1820 E. Newberry Street, Appleton, WI nearly every night over the collection period leading your affiant to conclude BESS is residing at 1820 E. Newberry Street.

33. On June 6, 2023, your affiant and ATF SA Frank Rutter conducted surveillance at 1820 E. Newberry Street, Appleton, Wisconsin. Prior to conducting surveillance agents reviewed photographs of BESS obtained through his social media accounts and DMV photograph. At approximately 1:46 pm cst, agents observed a black male, whom they immediately recognized as BESS step out of the door on the east side

of the residence. BESS walked around on the driveway while holding a phone. BESS remained outside for approximately three minutes before going back into the house through the east side door. It should be noted, the location data collected for (773) 220-3134, the phone associated with BESS, indicated the phone remained stationary all day, and was pinging on a cellular tower which covered 1820 E. Newberry Street shortly before agents observed BESS at the house.

34. On June 7, 2023, SA Rutter conducted surveillance at 1820 E. Newberry Street. At approximately 1:20 pm cst, SA Rutter observed BESS walk out of the eastern door of the house and walk to the end of the driveway. BESS grabbed the garbage can from the end of the driveway and walked it back to the house and he went back inside the house using the same east door. It should be noted, location data collected for (773) 220-3134, the phone associated with BESS, was pinging on a cellular tower that covered 1820 E. Newberry Street at the time SA Rutter observed BESS.

Search Warrant and Interview of Temaj BESS

35. On June 23, 2023, ATF executed a federal search warrant at 1820 E. Newberry Street in Appleton, Wisconsin, where agents located two Apple iPhones, a Samsung smartphone, a Glock pistol box, 7 rounds of 9 mm ammunition, and an unserialized Polymer 80 PF940C PMF pistol with attached auto switch. It should be noted, your affiant later function tested the PMF pistol with the auto switch and found it to function test as a machine gun.

36. During the execution of the search warrant, BESS was briefly placed in handcuffs while agents secured the residence for officer safety. Your affiant explained to BESS he was not under arrest but was being handcuffed temporarily while agents secured the residence. As soon

as the residence was deemed secure, BESS was removed from handcuffs. Once the residence was searched and deemed secure, your affiant asked BESS if he wanted to speak with agents outside the residence and he stated he did.

37. Once inside the vehicle, your affiant again reiterated to BESS he was not under arrest, and he was free to leave or stop answering questions at any time.

38. Your affiant began the interview by asking about a Taurus pistol (model G2C, 9 mm, with an obliterated serial number) which was located in the possession of Jeremiah RANDOLPH (B/M, DOB 03/17/2004) on March 16, 2023. BESS had previously spoken with Appleton Police Sgt. Michael Chevremont about this firearm. BESS stated RANDOLPH approached him and asked BESS to purchase a firearm for him. BESS stated he told RANDOLPH "I get guns all the time", and explained to RANDOLPH that he would go to the store to buy the firearm for him. BESS further explained RANDOLPH "thought I did it illegally". Your affiant interpreted that statement to mean RANDOLPH believed BESS acquired firearms from locations other than an FFL, which maintains mandatory records of all sales. BESS stated he asked RANDOLPH if he was in trouble and RANDOLPH said he was not in trouble. BESS stated he knew RANDOLPH was not 21 years old and could not purchase a firearm for himself. BESS stated RANDOLPH provided him money totaling the cost of the firearm plus \$100 (profit) for BESS to purchase the firearm on his behalf. BESS stated approximately 4 months after he purchased the firearm for RANDOLPH, he approached him and asked for the firearm back, at which point RANDOLPH told BESS that he "scratched off the serial number". BESS stated he knew RANDOLPH for approximately 4 years prior to buying a firearm for him. BESS stated RANDOLPH approached him to purchase the firearm because RANDOLPH knew BESS had previously obtained his concealed carry permit and posted videos

to his social media accounts depicting himself shooting firearms at the range.

39. BESS stated RANDOLPH went with him to purchase the firearm from “Mister Money” pawn shop, and RANDOLPH had previously told BESS the type of firearm he wanted BESS to purchase for him. BESS stated the firearm was a Taurus pistol but could not remember the specific model. BESS stated he used a Cash App debit card to pay the store for the firearm. BESS stated RANDOLPH paid him for the firearm using Cash App but could not remember if he paid him before or after he bought the firearm for RANDOLPH. BESS stated he gave the firearm to RANDOLPH right away after he purchased the firearm.

40. Your affiant asked BESS how many total firearms he has purchased, and he stated he has purchased approximately 7 firearms.

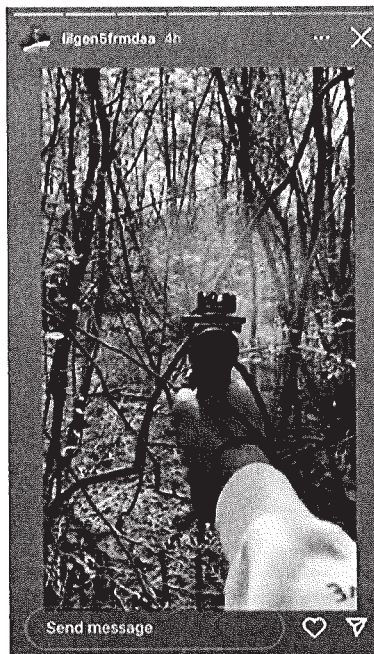
41. Your affiant then asked BESS about a firearm he purchased for Patrick A. WATSON (DOB 07/04/2001) on September 7, 2022. BESS stated WATSON approached him to purchase a firearm for him because he knew BESS had his concealed carry permit. BESS stated WATSON paid him \$100 (profit) to buy him the gun stating, “everyone was trying to give me a hundred for it.” BESS stated the firearm he bought for WATSON was a Glock 19 Gen 5 pistol and he purchased it at Pawn America in September of 2022. BESS stated WATSON went with him to purchase the firearm and he gave the firearm to WATSON immediately following the transaction. BESS stated WATSON paid him for the firearm in cash.

42. BESS stated he previously purchased a rifle for himself, but explained the firearm was seized by Neenah PD from a friend’s house “right after he got it”. BESS stated the friend was named “George BAGGETT”. Your affiant asked BESS how much time had elapsed between his purchase of the rifle and it’s seizure by the police, and he responded, “not even a day.” BESS stated Neenah PD told him BAGGETT was a convicted felon.

43. BESS stated the first firearm he ever purchased was on May 5, 2022, and that firearm was stolen in Milwaukee, Wisconsin during the filming of a rap video in which the firearm was being used as a prop. BESS stated this firearm was a Taurus G3C pistol which he purchased from Fleet Farm in Appleton, WI.

44. Your affiant asked BESS if there were any guns inside the residence at this time and he said “no”.

45. Your affiant asked BESS about his social media posts depicting himself holding firearms. BESS stated the photographs were old photos that he recently reposted. Your affiant then showed BESS the following photograph which depicted the hand of a black male apparently shooting a rifle in a forested location:



46. BESS stated this firearm belonged to his cousin, and stated he was the person shooting the firearm in the photograph. BESS could not remember where he was when he was shooting the firearm. BESS stated his cousin's name is "Darnell MCCISSICK" and he is 21 years old. BESS stated MCCISSICK lives in Appleton, WI.

47. BESS stated the other firearms he purchased for himself. BESS stated he would shoot the firearms a couple times and get bored with them, then he would sell them via “private sale”. BESS could not remember the names of the people he sold the remaining firearms. Agents asked BESS why people would approach him to purchase firearms, and BESS stated he had a reputation as being a “gun guy”. BESS stated he would often purchase a firearm knowing he would eventually sell the firearm when someone would inquire about a gun. BESS stated in those situations he would sell the firearm for the cost of the firearm plus \$100. BESS again reiterated that he has only purchased 7 firearms. BESS further explained he would take money from a previous sale and use it to fund the purchase of the next firearm he’d sell.

48. BESS stated he has resided at 1820 E. Newberry Street, Appleton, Wisconsin since January 2023, and he was living there because his mother kicked him out. BESS stated he is currently unemployed.

49. At this point, your affiant was notified by the search team inside the residence that they located a polymer 80 pistol (unserialized) with a glock auto sear installed. Your affiant asked BESS about the firearm, and he first said the firearm was not his, then he admitted he was the one who brought the firearm into the house. BESS stated he got the firearm the previous night, and stated he did not buy it. BESS then proceeded to tell agents he acquired the firearm after he broke into a vehicle and stole it. BESS stated, “I saw that it had a switch on it. I never had a gun with a switch on it before, and I stole it.” Once agents questioned this story and how he knew which car to target, he again changed his story.

50. BESS stated he got recently was arguing with a subject who made threats against BESS. BESS stated he was in fear for his safety, so he asked the source for a firearm to protect himself and the house. BESS stated he did not know it had an auto sear installed on it, and when

BESS realized the firearm had been converted to a machine gun, he intended to give it back. BESS stated he spoke with the source of the firearm over the phone. Agents explained to BESS that they would be searching his cellular phone and BESS acknowledged that pictures and messages pertaining to this firearm would be on his phone. BESS then changed his story and stated the source did state the firearm had a switch on it, but BESS said he did not believe it. Agents asked BESS if he was protecting the source of the machine gun because they are a family member, and he replied yes. Your affiant asked BESS if the source of the firearm was his cousin and he said yes but would not identify him.

51. At this point, BESS stated he did not wish to answer any more questions, and agents immediately terminated the interview.

Review Of BESS' Facebook Data

52. On August 28, 2023, your affiant reviewed data for the Facebook profile "Temaj BESS" (Facebook user ID# 100089599433619) which was obtained via a federal search warrant. Your affiant observed the registered phone number for the account is 773-220-3134, and the registered email address for this account was temaj.bess@icloud.com. It should be noted, your affiant has previously identified 773-220-3134 as belonging to BESS, and agents recovered two Apple iPhones in BESS' residence during the search warrant at his residence.

Conclusion

53. Your Affiant is aware through training and experience that it is common for those who possess and traffic firearms, to utilize electronic media devices, which often possess cameras, to photograph and send messages to negotiate the purchase and sale of their firearms.

54. Affiant is aware that those who possess Apple devices often utilize Apple's iCloud services to back up and store their data in the event they need to recover information. Further, affiant is aware that this stored data can include, but is not limited to, text messages, call records, location data, photographs and videos.

55. Affiant believes the correspondence located within the Target iCloud account will additionally provide further evidence of violations Title 18 U.S.C § 922(a)(6) (lying on an official form); and 924(a)(1)(A) (conspiracy).

BACKGROUND CONCERNING APPLE

56. In my training and experience I have learned, Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

57. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected

device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS.

Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.S

58. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

59. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to

and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

60. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple’s website. Apple also maintains records reflecting a user’s app purchases from App Store and iTunes Store, “call invitation logs” for FaceTime calls, “query logs” for iMessage, and “mail logs” for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

61. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user’s IP address and identifiers such as the Integrated Circuit Card ID number (“ICCID”), which is the serial number of the device’s SIM card. Similarly, the telephone number of a user’s iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address (“MAC address”), the unique device identifier (“UDID”), and the serial number. In addition, information about a user’s computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user’s web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including

communications regarding a particular Apple device or service, and the repair history for a device.

62. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

63. Your affiant is aware that Temaj BESS's iCloud account is likely to contain electronic information such as messages, call records, location data, photographs and videos. The account Temaj.bess@icloud.com and the evidence therein would accordingly be extremely useful to the investigation. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and

how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

64. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

65. In addition, the user’s account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

66. Account activity may also provide relevant insight into the account owner’s state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a

plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

67. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

68. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

69. There is probable cause to believe that in the Apple iCloud account for Temaj BESS listed as Temaj.bess@icloud.com as listed in the aforementioned paragraphs there is evidence of violations of 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 922(a)(1) (dealing firearms without a license), 18 U.S.C. § 922(a)(6) (lying and buying), 18 U.S.C. § 922(g)(1) (unlawful possession of firearms and ammunition by a convicted felon), 18 U.S.C. § 922 (k) (receiving/ship/transport of a firearm with an obliterated serial number), and 18 U.S.C. § 922 (o) (transfer or possession of machinegun).

70. That based upon Affiant's training and experience, Affiant knows that the execution of a search warrant related to remotely stored accounts such as Apple and within email accounts maintained by Apple such as "iCloud" usually results in items of

personal documents such as bills, bank statements, photographs, videos, and other items or documents which establish the identities of persons in control of the media.

71. That based upon Affiant's training and experience, Affiant knows that individuals purchasing and selling firearms routinely keep emails, regarding the purchases and/or sales.

72. That Affiant knows that it is common for firearms purchasers and possessors to maintain electronic records, receipts, notes, ledgers, receipts relating to the transportation, ordering and purchase of firearms and that such records are typically kept where the purchaser would have ready access to them including Apple accounts.

73. That Affiant knows that firearm possessors and traffickers often take or cause to be taken photographs and other visual depictions of themselves, their associates, their property and their firearms, and typically keep and maintain these photographs in their residences and other locations where they exercise dominion and control such as telephones, tablets, computers, other media storage devices and remote storage locations.

TECHNICAL TERMS

74. Based on my training and experience, I use the following technical terms to convey the following meanings:

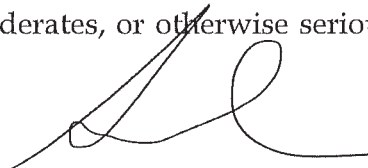
75. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from

its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

76. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

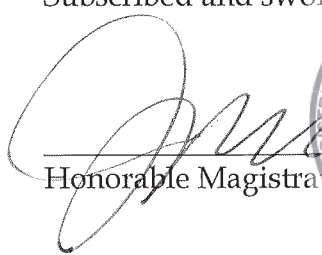
REQUEST FOR SEALING

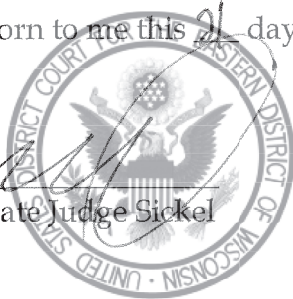
77. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.



Sean Carlson, ATF Special Agent

Subscribed and sworn to me this 21 day of September, 2023.



Honorable Magistrate Judge Sickel

ATTACHMENT A
Property to Be Searched

This warrant applies to information associated with Temaj.bess@icloud.com that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

ATTACHMENT B
Particular Things to be Seized

1. Information to be disclosed by Apple (Provider)

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserve, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A from 01/01/2022 to the present:

- All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses,

Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

- The contents of all emails associated with the account from 01/01/22 to present, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;
- The contents of all instant messages associated with the account 01/01/22 to present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

- The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;
- All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;
- All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;
- All records pertaining to the types of service used;

- All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and
- All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

Information to be seized by the government

1. All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 922(a)(1) (dealing firearms without a license), 18 U.S.C. § 922(a)(6) (lying and buying), 18 U.S.C. § 922(g)(1) (unlawful possession of firearms and ammunition by a convicted felon), 18 U.S.C. § 922 (k) (receiving/ ship/ transport of a firearm with an obliterated serial number), and 18 U.S.C. § 922 (o) (transfer or possession of machinegun), those violations involving Temaj BESS and occurring after 01/01/22, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Records containing the sale/purchase order of ammunition in a illegal format that is intended for the military/ law enforcement that would not be for public use. Records can be contained in emails, text messages, SMS messages, iMessages, etc.

- (b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- (e) The identity of the person(s) who communicated with the user ID about matters relating to the conspiracy and illegal importation of ammunition, including records that help reveal their whereabouts.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Apple Inc. ("Apple"), and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Apple. The attached records consist of _____ (pages/CDs/megabytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Apple, and they were made by Apple as a regular practice; and

b. such records were generated by Apple's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Apple in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Apple, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Signature